IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JENNIFER CLEMENS, individually and on behalf of all others similarly situated,

Plaintiff,

v.

EXECUPHARM, INC. and PAREXEL INTERNATIONAL CORP.,

Defendants.

CIVIL ACTION
NO. 20-3383

PAPPERT, J. **February 25, 2021**

MEMORANDUM

Jennifer Clemens, individually and on behalf of a purported class, sued ExecuPharm, Inc. and parent Parexel International Corporation over a data breach at ExecuPharm. Defendants moved to dismiss the Complaint pursuant to Federal Rule of Civil Procedure 12(b)(6), and the Court subsequently requested supplemental briefing from the Parties as to whether Clemens has standing to bring her claims. Having considered the supplemental briefing and for the reasons that follow, Clemens lacks standing and the Court does not have subject matter jurisdiction to address her claims.

I

A

i

Clemens worked at ExecuPharm from February to November of 2016 and provided the company "significant amounts of her personal and financial information" as a "condition of her employment." (Compl. ¶¶ 56–57, 59, ECF No. 1.) She signed an employment agreement "[a]s a further condition of her employment." (*Id.* at ¶ 58.) In

it, ExecuPharm agreed to "take appropriate measures to protect the confidentiality and security of all personal information." (*Id.*) Although Clemens left the company years ago, ExecuPharm retained her sensitive personal information until at least March 13, 2020. (*Id.* at ¶ 59.) On that date, ExecuPharm's server was hacked by the CLOP ransomware group. (*Id.* at ¶¶ 1, 11, 14, 31.)

CLOP organized a successful email phishing scheme to obtain server access and encrypt data by installing malware. (*Id.* at ¶ 13.) It accessed thousands of individuals' sensitive information, including full names, home addresses, social security numbers, taxpayer IDs, credit card and bank information, beneficiary information and, in some cases, passport copies. (*Id.* at ¶¶ 1–2, 4.) It then demanded a ransom from ExecuPharm in exchange for data decryption tools and threatened to release the data if the ransom was not timely paid. (*Id.* at ¶ 13.) On April 26, CLOP made at least some of the information it stole available for download on the "dark web." (*Id.* at ¶¶ 2, 15, 29). "[T]he download links contained nearly 123,000 files and 162 gigabytes of data, including nearly 19,000 files of correspondence involving ExecuPharm and Paraxel; more than 80,600 e-mail correspondences; financial, accounting, user documents of ExecuPharm's employees and managers; and a complete backup file of ExecuPharm's document management system." (*Id.* at ¶ 29.)

Clemens alleges she learned in an email from ExecuPharm on March 20 that her information was accessed during CLOP's data breach and ExecuPharm "confirm[ed]" in an April 26 email "that her family's most sensitive personal and financial [information] was 'shared on the dark web.'" (*Id.* at ¶¶ 60, 64.) In making these allegations, Clemens appears to rely on the ExecuPharm communications she quotes elsewhere in the

Complaint, which do not state she specifically was a victim of the data breach. According to the Complaint, ExecuPharm's March 20 email stated:

> Unfortunately, we now believe sensitive information has been accessed, including social security number, banking information (copy of a personal check for direct deposit), driver's license, date of birth, home address, spouse's name, beneficiary information (including social security numbers) and payroll tax forms (such as W-2 and W-4). For some employees, copies of passports also were accessed.

(Compl. ¶ 18.) The email appended a pdf of a March 18 letter to former employees, which explained to recipients "[i]f you are receiving this . . . we believe you *may be* among the group of former employees impacted by this incident." (*Id.* at ¶ 16 (emphasis added).) ExecuPharm's April 26 email stated it had "become aware that the information accessed by the cyberattackers has been shared on the dark web"—it does not appear to have said anything about Clemens's or her family's data specifically. (*Id.* at ¶ 30.) Notwithstanding the apparent inconsistencies in Clemens's allegations, the Court interprets the Complaint in the light most favorable to her and credits that her information was accessed and posted online.

ii

After the breach, ExecuPharm offered free identity monitoring services for one year to all potentially affected current and former employees. (*Id.* at ¶¶ 24, 65.) Clemens took advantage of these services, but also purchased additional services for herself and her family at a cost of $39.99 per month. (*Id.* at ¶ 71.)

Since the breach, Clemens "has spent significant time and effort reviewing her financial accounts, bank records, and credit reports for unauthorized activity and will continue to do so." (*Id.* at ¶¶ 61, 67–69.) She has occasionally missed work in order to pursue mitigative measures. (*Id.* at ¶ 70.) Once, after she changed her family's bank

account numbers, she was delayed from accessing her funds due to a mistake by the bank. (*Id.* at ¶ 69.) Clemens also says she sought and paid for counseling to cope with stress and anxiety caused by the breach. (*Id.* at ¶ 72.) She believes that "[g]iven the highly-sensitive nature of the information stolen, the value of [her] [p]ersonal [i]nformation has been diminished and she remains at substantial and imminent risk of future harm." (*Id.* at ¶¶ 73, 97.) But she does not allege she has experienced any identity theft or fraud. *See generally* (*id.*).

According to Clemens, many breach victims "have already experienced significant harms . . . including, but not limited to, identity theft, financial fraud, tax fraud, medical and healthcare fraud, unauthorized financial accounts or lines of credit opened in their names, and fraudulent payment card purchases." (*Id.* at ¶ 81.) Victims other than herself have also spent time, money and effort monitoring their accounts and protecting their information. (*Id.*)

B

Clemens sued ExecuPharm and Parexel on July 10, 2020 seeking relief individually and on behalf of a class of individuals whose personal information was compromised by the breach. (*Id.* at ¶ 100.) Her Complaint asserts claims of negligence (Count I), negligence *per se* (Count II), breach of implied contract (Count III) and breach of contract (Count IV) against both Defendants and breach of fiduciary duty (Count V) and breach of confidence (Count VI) against ExecuPharm. *See generally* (*id.* at ¶¶ 116–56). It also seeks a declaratory judgment stating Defendants' existing data security measures fail to comply with their duties of care and instructing Defendants to

implement and maintain industry-standard measures. (*Id.* at ¶¶ 157–61.) Defendants moved to dismiss the Complaint in full. *See* (Mot. to Dismiss 1, ECF No. 14).

On February 5, 2021, the Court ordered the Parties to provide supplemental briefing addressing whether Clemens has standing to bring her claims. (Suppl. Briefing Order, ECF No. 24.) In their Supplemental Brief, Defendants argue Clemens has not alleged an injury-in-fact sufficient to establish Article III standing in this Circuit. *See generally* (Defs.' Suppl. Brief 2–8, ECF No. 25). Clemens argues she has established standing for all claims, but contends "irrespective of her other claims," she "plainly" has standing for her contract-based causes of action. *See generally* (Pl.'s Suppl. Brief 3–10, ECF No. 26).

II

Article III of the United States Constitution limits the exercise of judicial power to cases and controversies. *See Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 408 (2013); *see also Taliaferro v. Darby Twp. Zoning Bd.*, 458 F.3d 181, 188 (3d Cir. 2006) ("Absent Article III standing, a federal court does not have subject matter jurisdiction to address a plaintiff's claims, and they must be dismissed."). The case-or-controversy requirement demands that plaintiffs "establish that they have standing to sue." *Clapper*, 568 U.S. at 408 (citing *Raines v. Byrd*, 521 U.S. 811, 818 (1997)).

To demonstrate Article III standing, a plaintiff must establish: (1) she suffered injury-in-fact; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to speculative, that the injury will be redressed by a favorable decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). To establish injury-in-fact, a plaintiff must show her injury was concrete and

particularized and actual or imminent. *Id.* at 560–61. "[A]n allegation of future injury may suffice if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (internal quotations and citation omitted). But "[a]llegations of 'possible' future injury simply aren't enough." *Bognet v. Sec'y Commw. of Pa.*, 980 F.3d 336, 348 (3d Cir. 2020).

III

Clemens does not have standing to bring this lawsuit because she has not alleged an injury-in-fact. She argues she has because (1) her claims that her personal information was stolen by professionals, held for ransom and posted to the dark web demonstrate harm is certainly impending; (2) she alleges actual harm from her time, money and effort to protect her information based on the imminent risks she faces; and (3) she alleges harm to her private contract rights, which confers standing even in the absence of additional harm. *See* (Pl.'s Suppl. Brief 2–3).

A

The Third Circuit Court of Appeals has held that "in the event of a data breach, a plaintiff does not suffer a harm, and thus does not have standing to sue, unless plaintiff alleges actual 'misuse' of the information, or that such misuse is imminent." *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 365 (M.D. Pa. 2015) (citing *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. 2011)). In *Reilly*, law firm employees sued the firm's payroll processing company in a putative class action after the payroll company suffered a data breach by an unknown hacker that "potentially gained access to personal and financial information". *See Reilly v. Ceridien Corp.*, No 10-5142, 2011 WL

735512, at *1–2 (D.N.J. Feb. 22, 2011); *Reilly*, 664 F.3d at 40. The payroll company maintained plaintiffs' personal and financial information, and plaintiffs alleged that because of the breach they faced an increased risk of identity theft, incurred costs to monitor their credit activity and suffered emotional distress. *See Reilly*, 664 F.3d at 40. Plaintiffs did not, however, allege they suffered identity theft or fraud after the breach. *See generally id.* The district court dismissed the case for lack of standing and the Third Circuit affirmed. *Id.* at 41.

The Third Circuit observed the *Reilly* plaintiffs had yet to suffer harm from the breach and held that "[i]n data breach cases where no misuse is alleged . . . there has been no injury." *Id.* at 45. "[I]ndeed," there is "no change in the status quo" in such cases—for example, plaintiffs' "credit card statements [looked] exactly the same today as they would have been had" the breach never occurred. *Id.* The court further found plaintiffs did not face imminent future injury and stated their risk of harm was particularly attenuated because it was "dependent on entirely speculative, future actions of an unknown third party." *Id.* at 42. It noted it could not ascertain plaintiffs' potential future injury "without beginning our explanation with the word 'if'" and concluded that "*if* the hacker read, copied and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will [plaintiffs] have suffered an injury." *Id.* at 43 (emphasis in original); *cf. Storino v. Borough of Point Pleasant Beach*, 322 F.3d 293, 297–98 (3d Cir. 2003) ("[O]ne cannot describe how [plaintiffs] will be injured without beginning the explanation with the word 'if.' The prospective damages described by [plaintiffs] as certain, are, in reality, conjectural.").

Clemens contends "[a]t least three key factual distinctions distinguish this case from *Reilly*" and demonstrate she faces a non-speculative, substantial and imminent future injury. (Pl.'s Suppl. Brief 4.) First, the Complaint is "significantly more developed regarding the mode and scope of the breach" than in *Reilly*. (*Id.*) Whereas in *Reilly* "all that [was] known" was a third-party "potentially gained access" to the plaintiffs' information and it was unclear "whether the hacker, read, copied, or understood" any accessed data, here it is known that experienced hackers intentionally accessed sensitive information and encrypted it. (*Id.* at 4–5.) Second, unlike in *Reilly* Clemens "clearly alleged" criminal intent behind CLOP's hack because CLOP "is notorious for seeking ransom payments in exchange for releasing stolen data." (*Id.* at 5–6.) Third, sensitive data was confirmed stolen in the ExecuPharm breach, and the Complaint details many ways in which the breach of sensitive information can cause harm. (*Id.* at 6.) Clemens asserts "[t]he risk of harm is particularly significant in this case—perhaps more than any other data breach case on record—because the stolen data was made openly available for download on the dark web where anyone could access it." (*Id.* at 6–7.) "Thus, the risk of misuse does not depend on the criminal intent of just one party, but rather hundreds or thousands of criminals who already have access to the data and can misuse it at their discretion." (*Id.* at 7 (emphasis removed).)

For purposes of constitutional standing based on imminent harm, Clemens proffers distinctions without a difference. Her future harm remains speculative, rather than certainly impending or at substantial risk of occurring, because it is still only ascertainable using the word "if"—*if* anyone actually downloaded her information from the dark web, *if* they attempt to use her information, and *if* they do so successfully, only

then will she experience actual harm. *See Reilly*, 664 F.3d at 43. The speculative nature of any future harm is underscored by the fact that nearly one year has passed since the ExecuPharm breach and Clemens has never claimed to be a victim of fraud or identity theft because of it. *See, e.g.*, *Storm*, 90 F. Supp. at 366–67 ("[E]ven if the hackers here were more skilled or 'malicious,' . . . the fact remains that the harm of misuse has yet to occur almost a year later, which undercuts the imminency argument."). In fact, Clemens acknowledges her "mitigative measures have so far been successful in warding off identity theft and fraud." (Pl.'s Suppl. Brief 8.)[1] Even if Clemens's risk of identity theft or fraud increased post-breach, "the Third Circuit drew a bright line—'allegations of an increased risk of identity theft resulting from a security breach are [] insufficient to secure standing.'" *In re Rutter's Inc Data Sec. Breach Litig.*, --- F. Supp. 3d ----, 2021 WL 29054, at *6 (M.D. Pa. Jan. 5, 2021) (quoting *Reilly*, 664 F.3d at 43).

B

Clemens's allegations that she continues to invest time, money and effort to protect her information do not give her standing either. She admits "the mitigative measures taken by the plaintiffs in *Reilly*," which included time and money

[1] CLOP's alleged criminal intent does not render Clemens's future injury imminent. *See Rutter's*, 2021 WL 29054, at *5 (allegations credit card information was stolen for purpose of committing fraud or selling to other criminals insufficient to establish standing based on imminent future harm). Clemens's reliance on cases outside the Third Circuit finding imminent injury-in-fact for hacks undertaken for criminal purposes are unpersuasive. (Pl.'s Suppl. Brief 6.) Clemens points out that *Reilly* "distinguished data breach cases finding standing where there was some indication the breach was for criminal purposes." But the two cases the court found distinguishable, *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007) and *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), were neither decided nor adopted by the Third Circuit. *See* (*Id.* at 4); *Reilly*, 664 F.3d at 43–44. Moreover, neither case "discussed the constitutional standing requirements and how they apply to generalized data theft situations" or made a determination regarding whether the alleged injuries were "certainly impending." *Id.* at 44.

expenditures, "were not actual injuries because they relied on speculative future harm that was not imminent." (Pl.'s Suppl. Brief 8.) Here, too, her expenditures do not establish she has suffered actual harm because she made them based on a speculative future risk of fraud or identity theft. *See Reilly*, 664 F.3d at 46 ("[C]osts incurred to watch for a speculative chain of future events based on hypothetical future criminal acts are no more 'actual' injuries than the alleged 'increased risk of injury' which forms the basis for [plaintiffs'] claims. . . . . That a plaintiff has willingly incurred costs to protect against an alleged increased risk of identity theft is not enough to demonstrate a 'concrete and particularized' or 'actual or imminent' injury."); *see also Rutter's*, 2021 WL 29054, at *6 ("Plaintiffs . . .allege only possible future injuries and prophylactic measures to avoid those potential injuries, neither of which confer standing in a data breach action brought in the Third Circuit."); *cf. Clapper*, 568 U.S. at 416 ("Respondents' contention that they have standing because they incurred certain costs as a reasonable reaction to a risk of harm is unavailing—because the harm respondents seek to avoid is not certainly impending.").[2]

i

Clemens appears to suggest she may have suffered actual harm, or injury-in-fact in some form, because "it cannot be maintained that her information has not been *misused*: it was stolen, held hostage by known criminals, and then published for trade

[2] Clemens also claims she sought counseling for her stress and anxiety, once experienced a delay in accessing funds and that the value of her personal information has diminished as a result of the breach. None of these allegations confer standing. *Reilly* declined to find plaintiffs' emotional distress established standing, *see* 664 F.3d at 44–46, and Clemens attributed her delayed access to funds to her own bank's error separate from Defendants or the breach. *See* (Compl. ¶ 69). Nor does Clemens allege any facts which could plausibly show a diminution in the "value of her personal information."

amongst data thieves." (Pl.'s Suppl. Brief 8 (emphasis in original).) She claims "[t]he Third Circuit has unequivocally held that 'unauthorized *disclosures* of information' have long been seen as injuries." (*Id.* (quoting *In re Horizon Healthcare Servs. Data Breach Litig.*, 846 F.3d 625, 638 (3d Cir. 2017)).) This argument mischaracterizes the law in data breach cases.[3]

Reilly refers to the "misuse" of information after a data breach exclusively as fraud or identity theft. *See Reilly*, 664 F.3d at 42 ("there has been no misuse of . . . information" unless or until plaintiffs' "speculation that the hacker[] (1) read, copied, and understood their personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [plaintiffs] by making unauthorized transactions in [their] names" comes to fruition). Since *Reilly*, courts in this Circuit have declined to find stolen data has been misused in the absence of fraud or identity theft. *See, e.g.*, *Rutter's*, 2021 WL 29054, at *6; *Storm*, 90 F. Supp. 3d at 366 (finding no allegation of misuse where plaintiffs "have not alleged that their bank accounts have been accessed, that credit cards have been opened in their names, or that unknown third parties have used their Social Security numbers to impersonate them and gain access to their accounts."); *cf. FTC v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 609, 623 (D.N.J. 2014) (finding plaintiff alleged misuse where complaint stated data breach led to "fraudulent charges on many consumers' accounts[] and more than $10.6 million in fraud loss"). No court in this Circuit has found that information was misused without such harm.

[3] In addition, the quote Clemens cites from *Horizon* is part of a discussion about cognizable injury in privacy torts, none of which she has alleged in her Complaint. *See* 846 F.3d at 638–39.

C

Clemens also cannot establish standing based on her allegations of harm to her private contract rights "irrespective of her other claims." *See* (Pl.'s Suppl. Brief 9). As Clemens acknowledges in her Supplemental Brief, "the Third Circuit has not directly weighed in on contractual standing" and thus has not held, as she suggests, that "a contractual breach *categorically* creates an Article III injury." (*Id.* at 10, 10 n.1 (emphasis in original).) Indeed, the presence of contractual claims have not been relevant to courts' analyses of standing in data breach cases in this Circuit. *See, e.g.*, *Reilly*, 2011 WL 735512 (Complaint alleging negligence, breach of contract, breach of the covenants of good faith and faith dealing, consumer fraud, and New Jersey state law violations dismissed); *Rutter's*, 2021 WL 29054, at *2 (Amended complaint alleging negligence, negligence *per se*, breach of implied contract, unjust enrichment and violations of Pennsylvania state law dismissed as to uninjured plaintiffs); *Storm*, 90 F. Supp. 3d 359 (Complaints alleging negligence, breach of contract and violations of Pennsylvania state law dismissed).

An appropriate Order follows.

BY THE COURT:

/s/ Gerald J. Pappert

GERALD J. PAPPERT, J.